CLAIMS

1. A method of generating an authentication for updating a mobile communications device's location to a second communications device, the mobile communications device being registered to a proxy server, the method comprising the steps of, at the time of performing the location update,

i. providing a first input from the proxy server and a second input from the second communications device to a first algorithm to generate a shared secret,

ii. using the shared secret as the authentication when transmitting the location update to the second communications device.

2. A method according to claim 1 wherein the first algorithm is a hash function and wherein the hash of the first and second random numbers is the shared secret.

3. A method according to claim 1 or 2, wherein the mobile communications device has a device address, the address being derived from a second algorithm using a cryptographic key associated with the mobile device as the input to the algorithm.

4. A method according to claim 3, wherein the second algorithm is a hash function and the hash of the cryptographic key is the device address of the mobile communications device.

5. A method according to claim 4, wherein the mobile communications device provides the device address and the cryptographic key to the second communications device and wherein the second communications device verifies the validity of the device address prior to providing the second input to the first algorithm.

6. A method according to claim 5, wherein the verification comprises the steps of: performing a hash of the received cryptographic key to obtain a digest, and comparing the digest of the hash function with the received address.

7. A method according to any one of claims 3 to 6, wherein the cryptographic key is a public key of an asymmetric key pair associated with the mobile communications device.

8. A method according to claim 7, wherein the second communications device sends an encrypted copy of the second input to the mobile communications device, the encryption being performed using the public key of the mobile device.

9. A method according to any one of the preceding claims, further comprising the steps of: using the shared secret as an input to a third algorithm, and obtaining an output from the third algorithm as the authentication.

10. A method according to any one of claims 1 to 9, wherein the authentication is a hash of the concatenation of the shared secret and the location update message.

11. A method according to claim 10, further comprising the step of transmitting the location update message together with the authentication to the second communications device.

12. A method according to claim 11, further comprising the step of the second communications device computing a hash of the concatenation of the shared secret and the received location update message for comparison with the received authentication.

13. A method according to claim 12, wherein if the said comparison is the same, the second communications device registers the new location of the mobile communications device and transmits any subsequent messages to the new location.

14. A method according to any one of the preceding claims, wherein the first input from the mobile communications device is a random number.

15. A method according to any one of the preceding claims, wherein the second input from the second communications device is a random number.

16. A method according to any one of the preceding claims, wherein the second communications device is mobile.

17. A method according to any one of claims 1 to 15, wherein the second communications device has a fixed inter-network address.